- A little social engineering goes a long way. Before setting foot inside the target, we knew what software they were running and how it worked. By using an easily accessible database (ostensibly for the use of engineers), we were able to pick our own target.
- Physical security is often an illusion that relies on deterrence and intimidation. This is insufficient to deter a dedicated attacker.
- Closed networks are far less secure than Internet-facing hosts once you've gained access to them.

Night Vision

Physical penetration testing can be challenging in many ways, however there is absolutely no doubt that the most difficult tests are those that are carried out at night when security personnel are unaware. A couple of years ago my team was invited to simulate an attack by intruders on a medium-sized business in the Netherlands. The assignment had come from Pieter de Vries, the managing director, and he wished to involve as few people as possible. For this reason, he visited us at our offices and explained why he wanted the test.

The Mission

The company (we'll call them Nederlabs BV) was a leader in the drug development industry and world leaders in the field of brain perfusion. This led to them being targeted in equal measure by competitors and animal rights groups. When I say animal rights, I'm not talking about the people who genuinely care about animals and don't eat meat. (I'm squarely in that category myself.) I am talking about groups that firebomb family homes of employees they perceive to support animal testing or those who dig up and steal the remains of relatives. In one instance, the brother of a postman delivering to a facility was beaten with pick-axe handles.

Competitors and animal rights extremists are two completely different threats that would need to be separately modeled. A competitor is likely to infiltrate someone into the facility as an employee. This is not likely to be an option for animal rights extremists whose modus operandi is direct or covert action and intimidation.

Our client was more worried about animal rights groups than corporate spies. The extensive background checks that prospective employees are subjected to had proved fairly reliable in weeding them out. The biggest concern was a night time raid on the premises because a previous raid to free laboratory animals was launched and aborted (primarily because

Nederlabs, being a modern facility, makes extremely limited use of animal testing).

We needed to come up with an attack scenario that took into consideration both the risk of activists breaching the facility at night and the potential for corporate espionage. Therefore we created an attack scenario with the following parameters:

- The intrusion should be at night (or at least night time entry should be a component of the test) and no other staff would be given advance notice it was happening.
- The primary goal was to gain access to the office of the managing director, bug his office and install key logging hardware on his workstation.
- Additionally, we would leave several small packages in key locations. These packages were nothing more than molded plastic but, for the purpose of this audit, they would be considered to be blocks of C4 plastic explosive.

Information Gathering

We were ready to begin the preliminary research phase of the project and at this stage the questions that I wanted to answer were:

- How big is the site and what physical controls are in place to prevent intruders from entering it?
- What other controls are in place, for example, where are cameras located, are motions detectors used, and so on?
- How many guards are present and what is their strategy?
- Are guard dogs used?
- Assuming all goes well, where is the managing director's office?
- What are the points of maximum impact to deploy 'explosives'?

According to Google Earth, the site was approximately 50,000 square meters in total, more or less what I was expecting. It was surrounded on three sides by acres of forest but the front of the building and the car park faced a busy main road on the other side of which, conveniently, sat a McDonald's restaurant and a gas station. This would be perfect for initial surveillance.

The initial surveillance was carried out in two phases. The first phase took place during the day and was intended to give us an idea of their basic security posture. The night time phase helped us determine how much

this security changed. We also wanted to determine guard placement and patrols but ultimately the question was one of strategy: Would it be better to break in or disguise ourselves and walk in the front door?

We sat outside the restaurant for a couple of hours drinking coffee and watching the site through binoculars. A lot of people came and went but we didn't see any security. They probably wouldn't do perimeter patrols during the day anyway. One thing did stand out though: despite the fact that there were cameras covering every conceivable angle and inch of the premises, they were a model that did not include night surveillance features. Unless the grounds were floodlit after dark, the cameras would be almost completely useless as anything other than a deterrent.

As it started to get dark, we decided to move a little closer and take a stroll around the site itself. They'd certainly picked a very nice spot, almost completely surrounded by woodland, which was of course very useful for us as we could get right up to the fence and still be on *Natuurmonumenten* land (owned by the society for nature conservation). The fence carried security warnings every few meters. The company outsourced to protect the site was a local outfit called Trustek Security, who'd been good enough to supply contact details.

The fence itself was about 3 meters high. It extended around the entire perimeter of the site and was capped with razor wire, as shown in Figure 9.6. Again, this was just for show. Razor wire is completely pointless if it sits on top of something you can easily cut through, in this case low-security, chain-link fencing.

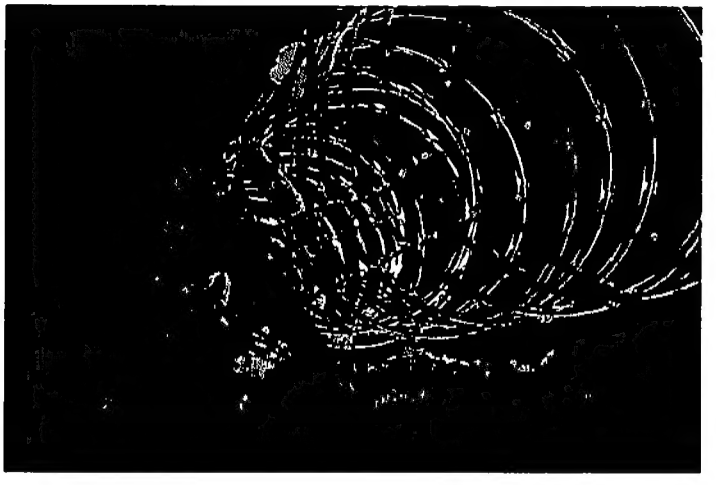

Figure 9.6 Coiled razor wire on chain link fencing looks intimidating but is easily defeated.

Razor Wire

Never be tempted to cut through razor wire itself. It is under tension (though this decreases with time) and rapidly uncoils if severed. Should you be standing next to it when this happens, you will suffer severe injuries.

Having determined that we could easily get into the facility, the question was how long we could remain undetected. There was no sign of flood lighting although the car park was lit. We were fairly convinced we could make it to the main buildings without being seen. The question then, of course, was how we would get in, remain undetected, and locate the boss's office. It was time to return to the office and do some more research.

We needed to learn a little more about the inside of Nederlabs so the next day we put in some time on the phone. The company was recruiting for various roles: marketing, sales, and scientists were all positions listed on their website. I decided that I'd put a CV together and apply for a job in bioanalysis.

Bioanalysis Job Advertisement

We are looking for both senior scientists and scientists to join our bioanalysis group.

Key areas of work within this bioanalysis laboratory are:

1. Development and validation of quantitative LC/MS/MS methods for the analysis of drug and metabolites in biological matrices.
2. Application of these methods to routine analysis of samples from pre-clinical and clinical studies.
3. Record-keeping in compliance with GLP/GCP.
4. Preparation of study plans and reports

Essential requirements for a scientist or senior scientist position are:

- Degree in chemistry or related subject or relevant experience
- Experience of chromatographic techniques i.e. HPLC, LC/MS and ability to problem solve
- Ability to take some science-based decisions without the need for referral

- Good written and verbal communication skills
- Computer literate
- Ability to work with minimum supervision and as part of a team
- Conscientious and meticulous in laboratory work
- Good time-management skills and ability to work to tight deadlines
- Highly motivated
- Willing to get involved with new ideas and initiatives

I'd been completely hopeless in chemistry at high school but I knew that scientists tend to have more of a rapport with each other than salesmen. (Sales people are naturally competitive even when working for the same company.) I figured I'd have a greater chance to look around the site and might even be able to get a tour as a job applicant. I swatted up the terms mentioned in the job specification (such as HPLC and GCP) and put together the sort of CV that would guarantee me an interview (sooner rather than later, I hoped). I fired off the CV with a covering letter oozing enthusiasm, called up Recruitment to make sure they'd received it and set about figuring out how we were going to execute the rest of the assignment.

Planning

The longer you remain on site during a physical penetration test, the greater your chances of discovery and failure become. It is therefore absolutely essential you conclude your operation as quickly as possible once the physical element is initiated. To this end, the more information you gather and the less uncertainty you have as you enter, the better. One of the goals of this assignment was to infiltrate the managing director's office and I wanted to know exactly where it was before I set foot in the building. The last thing you want is to be wandering around looking for something like that because it attracts unwanted attention. The Nederlabs HQ has five stories and it was a good bet that the head honcho's office was going to be on the top floor so I planned to apply a little social engineering to confirm this and maybe get some additional information while I was at it. I first searched the Web to find any companies that identified themselves as suppliers of Nederlabs, using much the same technique we deployed when hacking the SCADA network, and immediately hit pay dirt. Phemonex plc, a US supplier of laboratory equipment, list Nederlabs as a major client. As I browsed their website, I got a couple of SQL errors, which I couldn't help noticing. I could probably hack this web server easily, which would likely give me access to all sorts of information that would be useful to someone thinking about attacking Nederlabs.

Unfortunately, I wasn't allowed to do this but I made a note of the errors so that I could inform someone about it in the future. Next I needed to think up some way I could use Phemonex to get more information about the MD's office, so I grabbed some names from their website that I could use in a pretexting attack and called Nederlabs. The first call I made was pretty swift:

'Nederlabs, Goedemorgen. U spreekt met Vanessa Jannssen. Hoe kan ik u helpen?'

'Hello, can I speak to Pieter De Vries please?' I asked.

'Oh, er, I'm afraid he's not in the office right now actually he's on vacation, would you like to leave a message?' she replied, switching to English.

'No that's fine, I'll call him some other time,' I said and hung up.

I plugged in my Skype phone, told it to send my New York number as caller ID and called Nederlabs again.

'Nederlabs, Goedemorgen. U spreekt met Vanessa Jannssen. Hoe kan ik u helpen?'

'Good morning, do you speak English?' I said, putting on my best New York accent and hoping the receptionist wouldn't see straight through it. Most native English speakers certainly would. I made a mental note to practice my voices more.

'Certainly, how can I help you?' she replied obviously keen to show that she spoke excellent English as do all the Dutch.

'My name's Michael Rees. I'm calling from Phemonex,' I said.

'Ah, OK,' she replied, clearly familiar with the name, 'Who do you need?'

'Right, well, here's the thing. I'm coming to Holland in a couple of weeks to meet with Mr De Vries and I'm having a lot of trouble finding a hotel room. Apparently there's some kind of festival on.'

'Ah, yes,' she said, 'Carnaval. It's a Dutch religious festival.'

I was well aware that Carnaval was an alcohol-fueled week of mayhem that took place in the Netherlands every year and happened to coincide with the project. Quite what it had to do with religion was anyone's guess.

'That would explain it,' I said.

The receptionist gave me some suggestions on where to find a room and I asked, 'Is Mr. De Vries in the building?' Here was the crunch, either, as I was hoping, he was on vacation or the receptionist had just been told to say this.

'I'm sorry he's still in Spain, can I take a message for you?' she said.

'Ah, of course he is. Tell you what, would you mind giving me his extension? I'll call him before I leave for Amsterdam. I did have it, but it's with the rest of my Filofax, probably still in the back of a taxi in London.'

'Oh dear, OK. It's 424,' she replied.

'Thanks!'

Now you're probably thinking that that was an awful lot of work just to get someone's telephone extension. However, a lot of companies (certainly in the Netherlands) give numbers to rooms based on floor level – that is, 424 would be on the fourth floor. Telephone extensions in such companies are almost always the same as the room number. Following this logic and with a little luck, the MD's office is room 424, which was not as we had suspected, on the fifth floor.

I checked my email and discovered I had been invited for an interview on Monday. It was now Thursday and we had until the following Wednesday to complete the assignment. This was going to be tight. I wanted to use the interview as an opportunity to introduce our 'explosives' into or at least close to the laboratory facilities, which is why I would be angling for some kind of tour. The labs would likely be tightly locked down at night and, in any case, combining that with the penetration of the MD's office in one mission would take too long. The only problem was that I doubted I would be in the building for very long once they started asking me the technical interview questions. No matter how much I studied for them, it was unlikely I was going to fool anyone that I had a clue for very long. Social engineering was only going to get me so far.

It was time to determine when we were going to carry out the nighttime intrusion. Based on the information we had, we could choose to execute the mission on Sunday night prior to the 'job interview' or wait until Monday night in the hope that we might obtain further information that would be useful in the nighttime penetration. On balance, we decided to take the latter route; we still knew nothing about the interior of the building and anything I might discover on Monday could be potentially useful. Also, there were certain advantages to hitting the place on a week night in terms of the disguises we might be able to adopt when inside the facility. It is rare for employees in the Netherlands to go into work on the weekend, particularly on Sunday. It's not, however, rare for them to work late during the week. If we could get inside the building on Monday night and look the part, we would probably have less of a chance of being challenged by security. Therefore, it was determined that my goals when attending the Monday interview were as follows:

- Get an idea of the passes worn by permanent members of staff and if possible try and sneak out my guest pass.

- Determine how much reliance was placed on electronic key readers and how many we would be likely to have to pass to gain access to the fourth floor.
- Determine camera coverage within the public areas of the building.
- Take note of the general dress sense of staff in order to provide believable cover during the final penetration.
- Deploy 'explosives' in or as close to laboratory facilities as possible.

Carrying Out the Attack

Monday morning came around and I pulled into the guest car park in my rented car. Despite the elderly guard at the barrier, who just waved me through without challenge, I could detect no security presence so far. Inside reception things were a little different. Two guards stood by the gate to the lifts and once again there were a number of cameras. The girl at reception provided me with a standard paper guest pass in a plastic wallet (see Figure 9.7).

I was starting to wonder if my bag was going to be searched and I kicked myself that I hadn't considered this obvious possibility before. In it, I had a plastic block convincingly molded to look like Hollywood's idea of plastic explosive and a camera. If the guards clapped eyes on the contents, I doubted I would have time to show them my get-out-of-jail-free card before I was tasered. Luckily, there was to be no tasering that day. Five minutes later my contact for the interview arrived, shook my hand and swiped me through the gate.

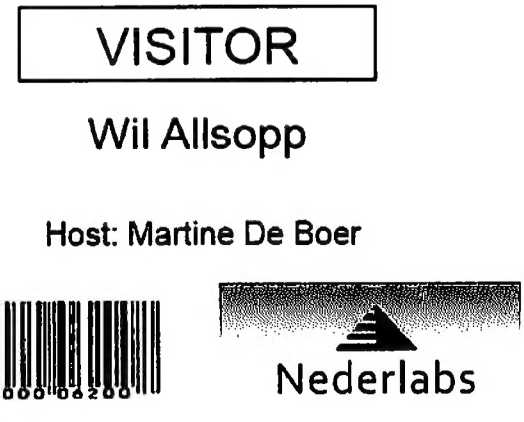

Figure 9.7 A standard visitor pass such as this is easy to replicate.

It wasn't long before I was able to answer one question: lab-coat chic was definitely the order of the day. We already had white lab coats so that at least wasn't going to be a problem. It looked like the interview itself was going to take place in a meeting room close enough to the labs that I could see scientists busying themselves with microscopes behind some glass doors. Those doors were swipe-card protected but none of the others we'd passed through had been. This boded well for the rest of the building. I excused myself momentarily to use the bathroom and used the opportunity to lift one of the foam tiles and hide one of my plastic blocks in the ceiling cavity.

The interview itself was pretty horrendous, with the interviewers exchanging glances a couple of times. I'm guessing they thought I was a journalist or an animal rights activist. In any case, I was ushered out of the building fairly quickly. I was able to hold on to my guest pass but I doubted it would be particularly useful. It didn't really matter; I had what I came for.

That night we prepared for the intrusion into the MD's office. One operator would be in his car across the road in permanent contact ready to cause a diversion if necessary. A colleague and I were going to perform the penetration and were dressed in white lab coats with suits and ties underneath. We all had the MD's home phone number on speed dial. Personally, I would have preferred the attack to go down differently; to con our way in at the front door but that's not what the rules of engagement called for.

At about 8:30 pm, we were outside the facility by the chain-link fence doing a last minute reconnoiter. It's good we did. From where we were crouching it was possible, thanks to the interior lighting, to see that a balcony on the second floor adjoined the café area inside. Directly below that, going all the way to the ground, was a drain pipe. If we were prepared to take a little risk, we might be able to get up the pipe right into the building. We agreed we'd go one at a time. If I was caught, then my colleague still had a chance to try something different but if I was successful I'd be able to watch out for him as he was coming up the pipe. Sometimes it's best to just go with a plan – think too much and you'd realize what a stupid idea it really was.

We cut a hole about 0.5 meters square in the chain-link fence. By that time it was dark enough and we were far enough from the cameras not to feel too concerned about anyone seeing us. I squeezed through and made a beeline for the drain pipe. It was now or never. It took me about 10 minutes to get up the pipe and my face level with the second floor. (I'm not 18 any more.) I could see a group of people inside the café but they weren't paying any attention to the balcony. I heaved myself up and

sat down on one of the chairs then signaled to my colleague that it was his turn. To my slight annoyance he made it up the pipe faster than I did but we grinned at each other over the coffee table. We got up and went to open the door into the café, which was locked. Now people *were* paying attention to us. One of the café staff opened the door and at looked at us more quizzically than suspiciously.

'Sorry, I didn't think anyone was out here,' he said, a little confused.

We left the café and went up the stairs to the fourth floor. It was about this time I realized that our hands (and our pristine lab coats) were covered in grime from the pipe. I put my hands in my pockets, which also had the effect of folding my lab coat out behind me. Problem solved. On the way we passed a couple of cleaning staff and someone in a suit who paid us no attention whatsoever. We found room 424 easily enough and one look at the lock told us we'd have no problem getting in *if* we weren't disturbed. The fourth floor appeared deserted, but that could change at any time. I called both the lifts and propped them open with chairs. Another chair under the door handle to the stair well might hold – we'd have to wait and see. My colleague, being the better locksmith, had already gone to work and a couple of minutes later he had the door open. I whipped the keyboard cable out of the back of the computer and attached the key logger. We were done.

As we closed the door to the office, we heard a commotion coming from the stair well; someone was trying to get in. With no time to relock the office, we legged it to the lifts, discarded one of the chairs and punched the ground-floor button. On the way down, we quickly debated our options: go out the front door or out of a window and back across the parking lot to the fence. We chose the former, which turned out to be the best option as the bored security guard barely glanced at us as we did our best to nonchalantly walk out of the gate and not panic and run. We crossed the road, got in the car and were away.

Conclusion

Protecting your staff and facilities from terrorists and bombers is virtually impossible. However, there are a few ways that Nederlabs could have been a little bit more secure.

- If you believe there to be a genuine risk that someone might bomb your building (as was the belief here) then search all guests, without exception. This includes job-interview candidates. A device that easily fits into a backpack is capable of wrecking devastation once brought inside, no matter where it's placed. Similarly, suspect packages should be examined by a fluoroscope before being opened.

- Unless cameras are specifically designed to work in low lighting, they are completely useless after dark. In this instance, every square foot of the premises should have been floodlit after dark.
- Razor wire, unless properly deployed, serves no purpose other than to make your site ugly. Solid high walls that extend deep enough into the ground to defeat tunneling are a much more practical alternative.
- We didn't wear ID badges in the building yet no one challenged us. Admittedly, it was late and there weren't many people around but this is no excuse. Always challenge anyone not wearing a badge and, if in doubt, call security immediately.

Unauthorized Access

Our last case study looks at a physical penetration test I did for a university in London. It may seem a little unfair to include a college; they're not exactly known for being high-security facilities, however this particular college hosted a powerful supercomputing center that was outsourced to do spatial modeling for the military, specifically to assess the effects of different classes of nuclear warheads in an urban environment modeled on the city. It unnerved me a little to know that such testing still goes on but at least these days it's modeled in computers rather than in actual urban environments.

Most of the university was just like any other: an open campus with stucco buildings and young idealistic students (who would probably freak if they knew the sort of research that took place under their noses). Tucked away from prying eyes a few select graduate students and government scientists were laboring away on a top-secret project. How *far* away from prying eyes was where we came in.

The Mission

It was an interesting assignment. We had three weeks to access data relating to the project on the IBM Bluegene and a completely open scope to do it. We were permitted to use any means we saw fit to gain access; after all, foreign intelligence services were unlikely to restrict themselves to a few port scans and other low-level hack attacks. Ultimately, physically penetrating the facility was likely to yield the best results.

Information Gathering

I wasn't familiar with the college at all, so the first step was to determine the most likely location of the supercomputer laboratory. This wasn't

difficult. There were three campuses: one specializing in drama and the arts, one for business management and one for the sciences – particularly computer science and high-energy physics (for which it had recently won a sizeable government grant). Well, it didn't take a rocket scientist to figure out the most likely candidate. I pulled up everything I could on the South End campus including satellite imagery and staff profiles.

There would be plenty of time to figure out the layout of the campus. I already possessed the requisite long hair and ripped jeans to pass as a student; however first I wanted to profile potential graduate students working on the project. This way we could attack other university systems such as human resources and student administration and pool all the information we needed to launch solid social-engineering attacks. We also needed to determine everything we could about their supercomputer: what it was called, where it was housed and how it was accessed over the network. The physics department website boasted that they had recently taken possession of a brand new IBM Bluegene named Deep Blue Thought. This I assumed was a pun on Deep Thought and Big Blue, references to the *Hitchhiker's Guide to the Galaxy* and IBM itself. This computer was high on the Top 500 list, where its military uses were openly stated (see Figure 9.8).

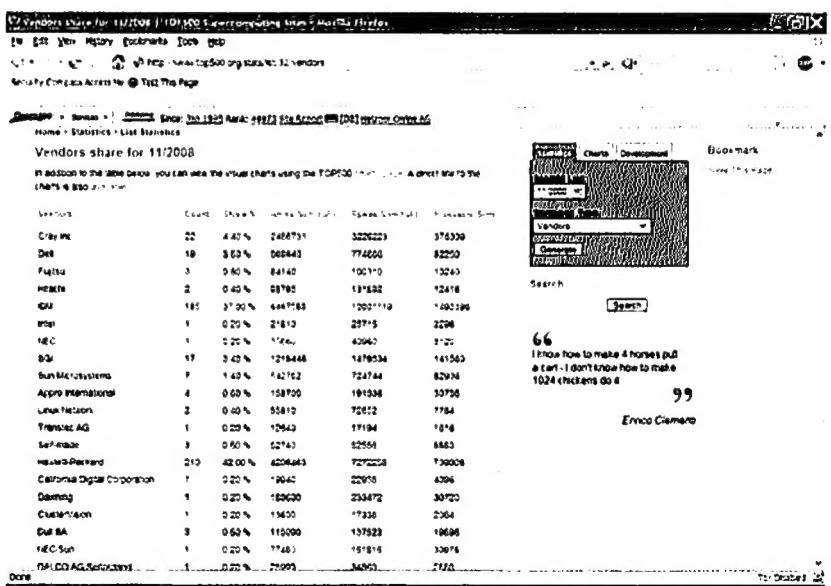

Figure 9.8 The TOP500 list maintains information about the most powerful computers in the world.